

United States District Court
Southern District of Texas
FILED

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

MAR 11 2019

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Alcatel TelCel Model 8050G phone
(further described in Attachment A)

David J. Bradley, Clerk of Court

Case No. B-19-mj-339

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Texas, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
21 U.S.C. § 841	Possession with intent to distribute a Schedule II controlled substance

21 U.S.C. § 846	Conspiracy to possess with intent to distribute a Schedule II controlled substance
-----------------	--

The application is based on these facts:

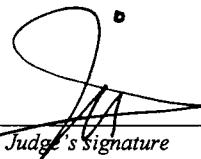
See Attachment C

- Continued on the attached sheet.
- Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Stephen Reuther, HSI Special Agent

Printed name and title


Judge's Signature

Ignacio Torteya III, United States Magistrate Judge

Printed name and title

Sworn to before me and signed in my presence.

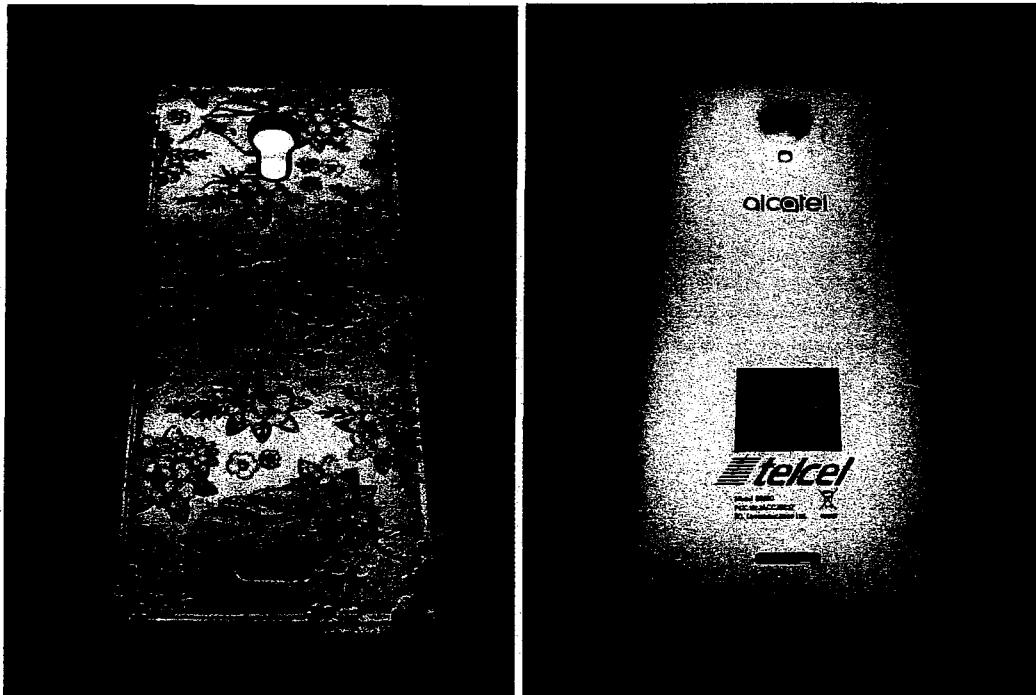
Date: March 11, 2019

City and state: Brownsville, Texas

ATTACHMENT A

PROPERTY TO BE SEARCHED

The cellular telephone that law enforcement found in SANCHEZ Marin's possession during this investigation is as follows:



A gold colored Alcatel TelCel Model 8050G cellular telephone bearing International Mobile Equipment Identity (IMEI) number, 014575006651561. This device, enclosed in a flowery unicorn phone case, is currently in secure evidence storage at the Homeland Security Investigations (HSI) Brownsville office located at 1800 Paredes Line Road, Brownsville, Texas.

This warrant authorizes the forensic examination of the cellular telephone for the purpose of identifying the electronically-stored information described in Attachment B.

ATTACHMENT B

ITEMS TO BE SEIZED

All records on the device described in Attachment A that relate to violations of 21 U.S.C. §§ 841, 846, including:

1. Lists of co-conspirator(s) and related identifying information.
2. Communication relating to the planning and carrying out of drug smuggling.
3. Types, amounts, and prices paid for drugs as well as dates, places, and amounts of specific transactions.
4. Any information related to the motivation for the drug smuggling [including names, addresses, phone numbers, or any other identifying information of unidentified co-conspirator(s)].
5. Any information related to the length and nature of the drug smuggling.
6. Any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information).
7. Any information recording Sandra SANCHEZ Marin's schedule or travel.
8. All bank records, checks, credit card bills, account information, and other financial records.
9. Social media data that identifies co-conspirator(s) or stores communication relating to the planning and carrying out of drug smuggling.
10. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
BROWNSVILLE DIVISION

IN THE MATTER OF THE SEARCH OF
AN ALCATEL CELLULAR
TELEPHONE LISTED IN
ATTACHMENT A, CURRENTLY
LOCATED AT 1800 PAREDES LINE
ROAD, BROWNSVILLE, TEXAS

Case No. B-19-mj-339

ATTACHMENT C

**AFFIDAVIT IN SUPPORT OF A SEARCH
WARRANT**

I, Stephen Reuther, a Special Agent with Homeland Security Investigations (HSI), being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations (HSI). I have been employed with HSI since June, 2017 and am currently assigned to the HSI Office of the Assistant Special Agent in Charge (ASAC), Brownsville, Texas, where I am a member of a group of Special Agents and Task Force Officers who specialize in the investigations of drug smuggling and money laundering within the White Sands High Intensity Drug Trafficking Area (HIDTA). Prior to my experience with HSI, I was employed as a major crimes detective and police officer in Florida since July, 2008.

2. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute arrest and search warrants issued under the authority of the United States. I have received training and participated in numerous investigations involving drug smuggling.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. As described in Attachment A, the property to be searched is an Alcatel Telcel, Model 8050G cellular telephone bearing IMEI 014575006651561. The device is currently in secure evidence storage at the HSI Brownsville office located at 1800 Paredes Line Road Brownsville, Texas.

5. The applied-for warrant would authorize the forensic examination of the device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

1. On January 20, 2019, HSI Special Agents assigned to the ASAC Brownsville White Sands HIDTA Task Force responded to the Brownsville and Matamoros Port of Entry (B&M POE) in reference to a call for assistance by US Customs and Border Protection Officers (CBPOs), who discovered an anomaly during the inspection of a 2005

Ford Lobo pickup truck, bearing Tamaulipas license plates [REDACTED] that was entering the United States from Mexico.

2. During the inspection and subsequent investigation, CBPOs discovered approximately 65.59 kilograms of methamphetamine mixture in liquid form contained within a non-factory compartment within the gas tank of the vehicle.

3. The driver and sole occupant of the pickup truck, Sandra SANCHEZ Marin, admitted during a post-Miranda interview with SAs that she conspired to deliver the vehicle, which she believed contained something illegal such as marijuana, to an unknown male at a busy, public location in Brownsville. After delivering the vehicle, the male was supposed to drive her to downtown Brownsville where she would exit the vehicle and then walk back to Matamoros via the pedestrian lane at a POE.

4. SANCHEZ Marin admitted she was to be paid approximately \$3,000 to deliver the vehicle to the male. SANCHEZ Marin also admitted she had been provided an upfront, partial payment and would be paid the remainder after she successfully delivered the vehicle.

5. SANCHEZ Marin was in possession of a single cellular telephone, an Alcatel Telcel, Model 8050G, which she identified as belonging to her. SANCHEZ Marin provided the agents with written consent to search her phone, which was searched in front of her

during the interview, as well as in the form of a logical extraction, the process of making a technological, partial copy of the information contained on the phone.

6. SANCHEZ Marin voluntarily provided the numeric password of her cellular phone to the agents.

7. SANCHEZ Marin provided the agents with phone numbers obtained from her phone, as well as directed agents to text messages on her phone that related to the person she was supposed to meet and deliver the vehicle to.

8. SANCHEZ Marin also told the agents she was supposed to send a text message to the person she was delivering the vehicle to after she successfully entered the United States from Mexico.

9. SANCHEZ Marin confirmed the identity of a person involved in the conspiracy using SANCHEZ Marin's Facebook profile, accessed through an application run on SANCHEZ Marin's cellular telephone.

10. Federal prosecution of SANCHEZ Marin was accepted and as a result, she was arrested for violations of 21 U.S.C. §§ 841 and 846.

11. Your affiant knows that drug smuggling is often a conspiratorial crime. Individuals involved in these activities often use cellular telephones to communicate with others who may act in different capacities and assist in the commission of the offenses. The cellular telephone was recovered in the possession of SANCHEZ Marin and it is likely it contains electronic records relating to the offenses and information that can lead to the identification of co-conspirators.

12. The cellular telephone is currently in the lawful possession of the HSI. The device was turned over to the HSI hours after being detained by the U.S. Customs and Border Protection during SANCHEZ Marin's entry into the U.S., subjecting the device to a possible border search. Therefore, while HSI may already have all necessary authority to examine the device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the device will comply with the Fourth Amendment and other applicable laws.

13. The device is currently in storage at the HSI Brownsville office located at 1800 Paredes Line Road, Brownsville, Texas. In my training and experience, I know that the device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the device first came into the possession of the HSI.

14. Though a logical extraction of the cellular telephone device was conducted, your affiant is aware of other methods, such as a physical extraction of the device, that yields a more complete copy of information on the device, including the possibility of retrieving deleted data.

TECHNICAL TERMS

15. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Cellular telephone: A cellular telephone is a handheld wireless device used for voice and data communication through radio signals. These telephones send

signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A cellular telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, cellular telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cellular telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Logical extraction: A logical extraction of data is performed through the device's designated Application Programming Interface (API). Upon connection, UFED 4PC loads the relevant API to the device. UFED 4PC then makes read-only API calls to request information from the device. The device replies to these API requests and extracts designated content items from the device's operating system. This process enables the acquisition of most of the live data in the device which is presented in a readable format and obtained in a forensically sound manner. Retrievable data types using a logical extraction

include passwords, call logs, SIM deleted call logs, device information, phonebook entries, SMS, images, videos, audio files, and application data.

c. Physical extraction: A physical extraction provides a bit-by-bit copy of the entire flash memory of a mobile device. This extraction method not only enables the acquisition of intact data, but also data that is hidden or has been deleted. Supported data types obtained using physical extraction include intact and deleted passwords, installed applications, geo tags, location information, media files such as photos and videos taken by the user, GPS fixes, emails, and chats.

16. Based on my training, knowledge and experience, I know that the cellular telephone has capabilities that allow it to serve as a telephone, digital camera, portable media player, GPS navigation device, and personal digital assistant. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

17. Based on my training, knowledge, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

18. *Forensic Evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct

evidence of the crimes described on the warrant, but also forensic evidence that establishes
8L 3/11/19
how the device~~s~~ ^{was} used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device~~s~~ because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

20. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

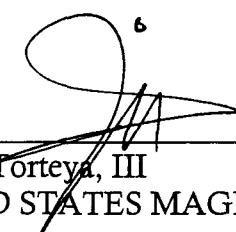
21. Based on the foregoing, I believe the cellular telephone contains evidence of violations of 21 U.S.C. §§ 841 and 846. Additionally, I believe that there is probable cause to believe evidence of those crimes, as more particularly described in Attachment B, will be found within the device. Accordingly, I respectfully request that the Court issue a warrant authorizing the search of the cellular telephone, which is more particularly described in Attachment A, for evidence of the above crimes, as more particularly described in Attachment B, within fourteen (14) days of the issuance of the requested warrant.

Respectfully submitted,



Stephen J. Reuther II
Special Agent
Homeland Security Investigations

Sworn to and subscribed before me
This 11th day of March, 2019.



Ignacio Torteya, III
UNITED STATES MAGISTRATE JUDGE